

A Secure Web-Based File Exchange Server Software Requirements Specification Document

CIISE Security Investigation Initiative

Represented by:

Serguei A. Mokhov

Marc-André Laverdière

Ali Benssam

Djamel Benredjem

`{mokhov,ma_laver,d_benred,al_ben}@ciise.concordia.ca`

Montréal, Québec, Canada

December 14, 2005

Contents

1	Introduction	2
1.1	Purpose	2
1.2	Scope	2
1.3	Definitions and Acronyms	3
2	Overall Description	5
2.1	Product Perspective	5
2.1.1	System interfaces	5
2.1.2	User Interfaces	5
2.1.3	Hardware Interfaces	5
2.1.4	Software Interfaces	6
2.2	Product Functions	6
3	Specific Requirements	7
3.1	Functional Requirements	7
3.1.1	Domain Model	7
3.1.2	Use Case Model	7
3.2	Software System Attributes	9
3.2.1	Security	9
3.2.2	Reliability	9
3.2.3	Availability	10
3.2.4	Maintainability	10
3.2.5	Portability	10
3.3	Logical Database Requirements	10
	Bibliography	11

List of Figures

3.1	SFS system packages	8
3.2	Normal user use-case	8
3.3	Administrator use-case	9

Chapter 1

Introduction

Building Trust is the basis of all communication, especially electronic one, as the identity of the other entity remains concealed. To address problems of trust, authentication and security over the network, electronic communications and transactions need a framework that provides security policies, encryption mechanisms and procedures to generate, manage and store keys and certificates.

This software requirements specification (SRS) document demonstrates all the concerns and specifications of the secure web-based file exchange server (SFS). SFS is a security architecture that we propose here to provide an increased level of confidence for exchanging information over increasingly insecure networks, such as the Internet. SFS is expected to offer users a secure and trustworthy electronic transaction.

1.1 Purpose

The intent of implementation and deployment of SFS facilities is to meet its basic purpose of providing Trust. Presently, SFS needs to perform the following security functions:

- *Mutual authentication of entities taking part in the communication:* Only authenticated principals can access files to which they have privileges.
- *Ensure data integrity:* By issuing digital certificates which guarantee the integrity of the public key. Only the public key for a certificate that has been authenticated by a certifying authority should work with the private key possessed by an entity. This eliminates impersonation and key modification.
- *Enforce security:* Communications are more secure by using SSL to exchange information over the network.

1.2 Scope

SFS is implemented to secure sensitive resources of the organization and avoid security breaches. The SFS allows trustworthy communication between the different principals. These principals must be authenticated and the access to the resources (files) should be secured and regulated. Any principal wants to access to the database needs to perform the following steps:

- *Mutual authentication:* The Web Server via which the database is contacted authenticates the principal using its digital certificate and username to ensure that it is who it claims to be . The principal authenticates also the server using its certificate information.
- *Principal validation:* To validate the principal, the server looks up information from an LDAP server which contains the hierarchy of all principals along with certificates and credentials.
- *Enforcing security:* The security is enforced by using SSL to communicate between the Web Server and the LDAP server, the Web Server and the database and between the principal and Web Server.
- *Principal authentication:* Upon successful authentication, the Web Server will allow the principal to perform actions on the database according to a pre specified Access Control List.
- *Kinds of principals:* There are two kinds of principals, administrators and clients: *Clients* have the ability to upload, download, delete and view files. *Administrators* have the ability to: Upload, download, delete and view files; Add, delete and modify users; Generate user's certificate, with all required information; Generate ACL to users; Manage groups, Perform maintenance.

Finally, this infrastructure allows additional features such as the ability to assign users to groups in order to provide users with the access to files prepared by other group members.

1.3 Definitions and Acronyms

- PKI: Public Key Infrastructure
- OpenLDAP : is a free, open source implementation of the Lightweight Directory Access Protocol (LDAP).
- OpenSSL: an open source SSL library and certificate authority
- Apache Tomcat: A Java based Web Application container that was created to run Servlets and JavaServer Pages (JSP) in Web applications
- PostgreSQL: An open source object-relational database server
- SSL: Secure Socket Layer
- JSP: Java Server Pages
- JCE: Java Cryptography Extension
- API: Application Programming Interface
- JDBC: Java Database Connectivity
- JNDI: Java Naming and Directory Interface
- LDAP: Lightweight Directory Access Protocol
- X.509: A standard for defining a Digital Certificate used by SSL
- SRS: Specification Request Document
- SDD: Specification Design Document

- DER: Distinguished Encoding Rules
- Mutual Authentication: The process of two principals proving their identities to each other
- SFS: Secure File Exchange Server, this product
- COTS: Commercial Off The Shelf, common commercially or freely available software

The coming sections of the SRS are a description of all the requirements to be implemented in SFS system. The requirements specifications are organized in two major sections: Overall Description and Specific Requirements.

Chapter 2

Overall Description

In this chapter we provide an overall insight of the general factors that affect the SFS system and its requirements.

2.1 Product Perspective

The SFS system is intended to operate in a distributed environment: clients machines, application server, database server, and LDAP server. SFS is accessed via secure connections we intend to provide in this work. The system's user can be either a normal user or an administrator. A normal user has the ability to upload, download, delete and view files. An administrator is able to: Upload, download, delete and view files; add, delete and modify users; generate user certificates along with all required information; generate an ACL to each and every user; manage groups; perform various maintenance actions such as: check log files, delete files, etc.

2.1.1 System interfaces

The various parts of the SFS application will be installed on client machines and different servers. The client that uses the system has to have the certificate installed on his machine to provide client authentication. The servers are responsible of one of the following functions: provide the database, provide the LDAP server functionalities, and provide the application server for different clients.

2.1.2 User Interfaces

The user interfaces consist of web-based graphical components that allow the user to interact with the SFS system. The user will use a web browser to send and receive data. If the user is the administrator, s/he will have more options to add, delete, etc. users, generate users certificates, generate ACL for each user, etc.

2.1.3 Hardware Interfaces

The hardware interfaces will be achieved through the abstraction layer of the Java Virtual Machine (JVM). The keyboard and the mouse are examples of such hardware interfaces that allow users to interact with the SFS system.

2.1.4 Software Interfaces

Among the most important software interfaces used in this project, we have:

- The SFS system is OS-independent due to the cross platform Java implementation. It will support web browsers such as Internet Explorer, Mozilla Fireworks, etc.
- Access to databases will be provided by JDBC 3 on both Windows and Linux environment.
- JXplorer? will be used to provide a graphical access to LDAP server.
- OpenLDAP? is used to host users' certificates.
- Java 1.5 JDK from Sun.
- JRE 1.5 from Sun.
- Servlets for client and administrator interfaces.
- Apache Tomcat5 server as the web server used in this project.
- PostgreSQL? is the database used to host users information, files, etc.
- OpenSSL toolkit to generate the certificates for users.

Hereafter, we provide the software and documentation's locations related to these interfaces:

- OpenLDAP? software and documentation found at: <http://www.openldap.org/>
- PostgreSQL database and documentation found at: <http://www.postgresql.org/>
- Java development kit 1.5 available at: <http://java.sun.com/j2se/>
- JSP documentation found at: <http://java.sun.com/products/jsp/>
- OpenSSL Toolkit found at: <http://www.openssl.org/>
- Apache Tomcat 5.0 web server found at: <http://tomcat.apache.org/>

2.2 Product Functions

The SFS system will implement the following functionalities:

- *Server authentication:* This use case allow the user to authenticate the web server is connecting to.
- *Client authentication:* This is use case allow the server to authenticate the user he is trying to connect to.
- *Secure communication:* Between users over the network.
- *Files handling:* Such as downloading, uploading, and deletion files.
- *Users management:* Administrator has the ability to add and delete users, add and delete groups, and assign users to groups.

Chapter 3

Specific Requirements

In this section we describe the software requirements to design the SFS system. The system design should satisfy the following requirements.

3.1 Functional Requirements

Hereafter, we express the expectations in terms of system functions and constraints. This includes the domain model and the most important use case diagrams of the SFS system.

3.1.1 Domain Model

The SFS system domain model consists of many packages.

- *Client authentication module*: used to provide users the ability to authenticate the server.
- *Server authentication module*: used to provide the server the ability to authenticate the clients.
- *LDAP connection module*: used to provide connection to the LDAP server in order to check clients' credentials.
- *Database connection module*: used to provide users the ability to connect to the database server in a secure mode.

3.1.2 Use Case Model

The SFS system consists of a set of use cases manageable by the users of the application. There are two types of users of the system: normal users and administrator. Normal can view, delete, download, and upload files. For the administrator, s/he can: add, delete, etc. users; generate users' certificates; generate ACL for each user, etc.

The diagram in Figure 3.2 shows the capabilities of a normal user.

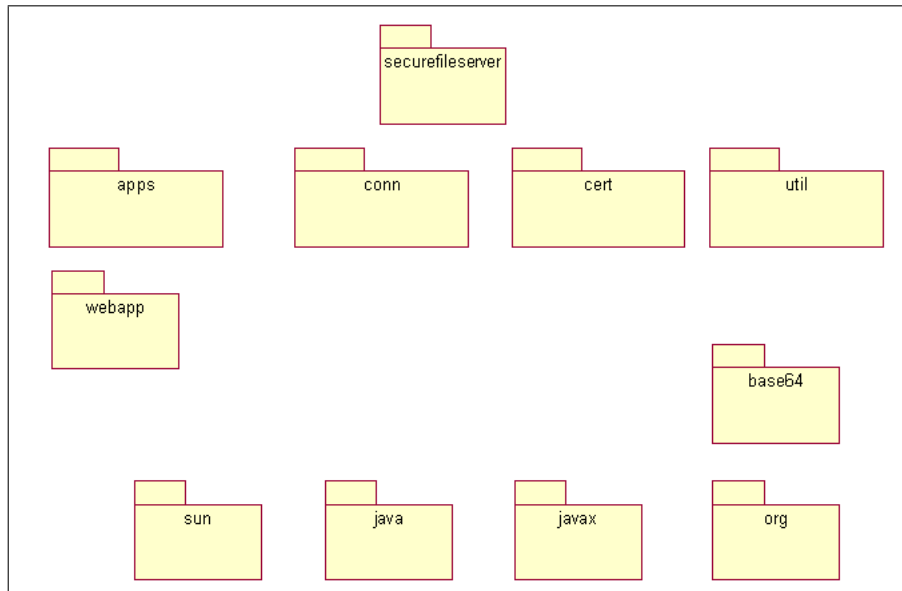


Figure 3.1: SFS system packages

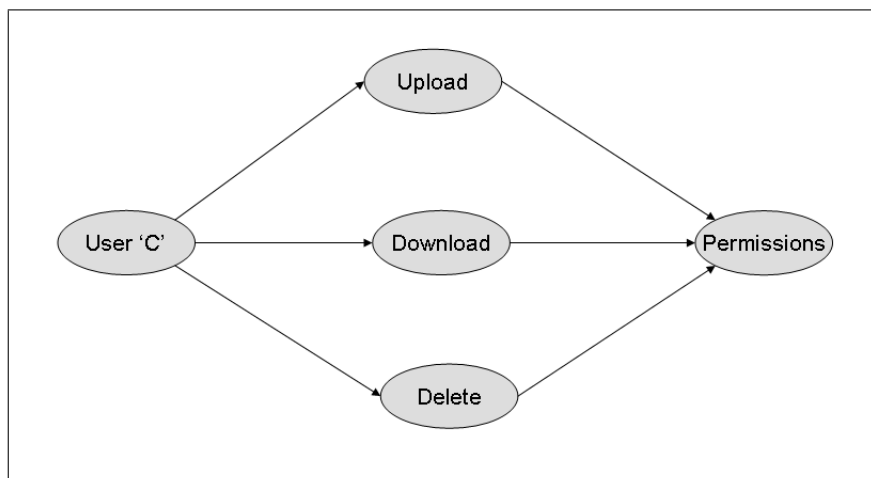


Figure 3.2: Normal user use-case

The diagram in Figure 3.3 shows the capabilities of the administrator user.

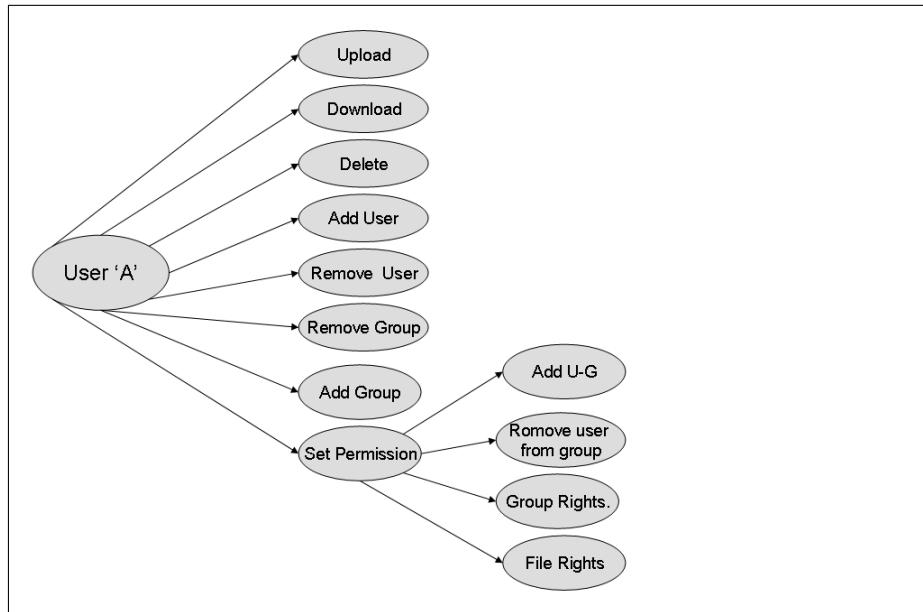


Figure 3.3: Administrator use-case

3.2 Software System Attributes

There are a number of software attributes that can serve as requirements. It is important that required attributes be specified so that their achievement can be objectively verified. The following items are some of the most important ones: security, reliability, availability, maintainability, and portability.

3.2.1 Security

Security is the most important attribute of the SFS design and implementation. The mutual authentication between the server and clients is crucial for the system use. The system should be able to authenticate users and differentiate among them, either are normal users or administrator. In order to achieve the security feature expected from the SFS system, the following tasks have to be realized:

- Utilize cryptographic techniques
- Check users' credentials before using the system and accessing the database
- Provide secure communications between different parts of the system

3.2.2 Reliability

The basis for the definition of reliability is the probability that a system will fail during a given period. The reliability of the whole system depends on the reliability of its components and on the reliability of the communication between its components. The SFS system is based mainly on some standard components such as OpenLDAP, OpenSSL,

JDBC, PostgreSQL, etc. The reliability of these service components is already proved. This fact improves the reliability of the system and restricts the proof work on assuring only of the reliability of the added components and the communications between the different components. In addition, the system must ensure the security of the communications which is the most important issue of the SFS system.

3.2.3 Availability

The SFS system must be able to work continuously in order to provide users with an access to different server's parts of the system. However, since this system depends on distributed information systems and databases, many constraints should be taken into account such as:

- The connection to the web server that provides access to the system
- The interconnection between different parts of the system should always be available; otherwise, the users cannot complete their tasks using the system.
- The database should be available in the database server side
- The LDAP server should be always available in order to check users' credentials
- The web server should be also available in order to allow users connecting to the system.

3.2.4 Maintainability

Maintainability is defined as the capacity to undergo repairs and modifications. The main goal in designing SFS system is to keep it easy to be modified and extended.

3.2.5 Portability

The portability is one of the main specifications of Java. Since SFS is implemented using the Java programming language, the portability is automatically satisfied and the system is able to run on any machine or operating system which supports the execution of a Java virtual machine.

3.3 Logical Database Requirements

The rationale behind SFS system is to provide secure connections for users accessing databases to view, delete, upload, and download files through a web server and LDAP server. After analyzing the requirements we propose using a relational database model to meet our requirements. This database is required to store information about users, files, groups of users, etc. The database is expected to work on 24 hours and 7 days in order to provide nonstop access to the users. Therefore, backup of the database should be taken periodically (daily or weekly). The relational database itself guarantees the flexibility, simplicity and elimination of redundancy once designed carefully. The entity relationship model will be elaborated in detail in the database design of the design part, in this document.

Bibliography

- [Apa11] Apache Foundation. Apache Jakarta Tomcat. [online], 1999–2011. <http://jakarta.apache.org/tomcat/index.html>.
- [CBH03] Suranjan Choudhury, Katrik Bhatnagar, and Wisam Haque. *Public Key Infrastructure, Implementation and Design*. NIIT Books, 2003.
- [Deb05] Mourad Debbabi. INSE 6120: Cryptographic protocols and network security, lecture notes. Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada, 2005. <http://users.encs.concordia.ca/~debbabi/inse6120.html>.
- [E⁺11] Eclipse contributors et al. Eclipse Platform. eclipse.org, 2000–2011. <http://www.eclipse.org>, last viewed February 2010.
- [GB11] Erich Gamma and Kent Beck. JUnit. [online], Object Mentor, Inc., 2001–2011. <http://junit.org/>.
- [Lar06] Craig Larman. *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development*. Pearson Education, third edition, April 2006. ISBN: 0131489062.
- [Leu05] Leuven Universitair. A few frequently used SSL commands. [online], Leuven Universitair Dienstencentrum voor Informatica en Telematica, 2005. http://shib.kuleuven.be/docs/ssl_commands.shtml.
- [Ope05a] OpenLDAP Community. OpenLDAP: The open source for LDAP software and information. [online], 2005. www.openldap.org.
- [Ope05b] OpenSSL Community. OpenSSL: The open source toolkit for SSL/TLS. [online], 2005. <http://www.openssl.org>.
- [O’R05a] O’Reilly. Home of `com.oreilly.servlet`. [online], 2005. <http://servlets.com/cos>.
- [O’R05b] O’Reilly. JXplorer – a Java LDAP browser. [online], 2005. <http://sourceforge.net/projects/jxplorer/>.
- [Sun05a] Sun Microsystems, Inc. Java servlet technology. [online], 1994–2005. <http://java.sun.com/products/servlets>.
- [Sun05b] Sun Microsystems, Inc. JavaServer pages technology. [online], 2001–2005. <http://java.sun.com/products/jsp/>.
- [The11] The PostgreSQL Global Development Group. PostgreSQL – the world’s most advanced open-source database. [ditigal], 1996–2011. <http://www.postgresql.org/>, last viewed January 2010.